UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JENNIE WHALEN, individually and on behalf of all others similarly situated, Plaintiffs, v. **NEW YORK UNIVERSITY,** Defendant.	Case No. **CLASS ACTION COMPLAINT** PROPOSED CLASS ACTION

Plaintiff Jennie Whalen, individually and on behalf of the Class defined below of similarly situated persons ("Plaintiff and Class Members"), alleges the following against Defendant New York University ("Defendant" or "NYU"). The following allegations are based on Plaintiff's knowledge, investigations by Plaintiff's counsel, facts of public record, and information and belief:

NATURE OF THE ACTION

1. NYU is the largest private research university in the United States, educating over 65,000 students.

2. Plaintiff and Class Members consist of former applicants, current students, and alumni of NYU. Plaintiff and Class Members were required to entrust NYU with their sensitive, non-public PII. Defendant could not operate or provide its services without gathering Plaintiff's and Class Member's PII, and retains it for several years.

3. The data that NYU exposed to the public is unique and highly sensitive. For one, the exposed data included personal identifying information ("PII"), like names, test scores, majors, ZIP codes, citizenship statuses, application statuses of the student (e.g., rejection), financial aid information, and financial details (collectively "Private Information").

4. Plaintiff and Class Members provided this information to NYU with the understanding NYU would keep that information private in accordance with applicable law.

5. On March 22, 2025, hackers took control of NYU's website by replacing the NYU homepage with charts and links containing sensitive Private Information of Plaintiff and Class Members that the hackers stole, resulting in injuries to Plaintiff and Class Members ("Data Breach"). The exposed information dates back to at least 1989.[1]

6. Upon information and belief, over 3 million individuals had their Private Information compromised as a result of the Data Breach.[2]

7. On March 27, 2025, Defendant posted a message to the NYU Community, stating that "someone accessed NYU's IT systems without authorization and took control of the systems that direct web traffic to NYU's website. For a period of about three hours, traffic to the www.nyu.edu website was instead directed to a webpage that the unauthorized actor posted on GitHub."

8. NYU spokesperson, John Beckman, "confirmed the 'malicious hack' and stated that law enforcement has been notified."[3]

9. NYU disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. NYU's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

---

[1] Dharma Niles, *Krish Dev & Yezen Saadah, Over 3 Million Applicants' Data Leaked on NYU's Website*, Wash. Square News (Mar. 22, 2025), https://nyunews.com/news/2025/03/22/nyuwebsite-hacked-data-leak/. (last accessed Apr. 8, 2025)

[2] *Id*.

[3] *Message to the NYU Community about the March 22, 2025, Cybersecurity Incident*, N.Y.U. News (Mar. 27, 2025), https://www.nyu.edu/about/newspublications/news/2025/march/memorandum-on-cybersecurity-incident.html. (last accessed Apr. 8, 2025).

10. Exacerbating the injuries to Plaintiff and Class Members, NYU failed to provide timely notice to Plaintiff and Class Members, depriving them of the chance to take speedy measures to protect themselves and mitigate harm.

11. Today, the Private Information of Plaintiff and Class Members continue to be in jeopardy because of Defendant's actions and inactions described herein. Plaintiff and Class Members now suffer from a heightened and imminent risk of fraud and identity theft for years to come and now must constantly monitor their financial and other accounts for unauthorized activity.

12. The PII exposed in the Data Breach can enable criminals to commit a litany of crimes. Criminals can open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members' individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

13. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit

freezes/unfreezes; (j) anxiety, annoyance, and nuisance; (k) continued risk to their Private Information, which remains in NYU's possession and is subject to further breaches so long as NYU fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information; and (l) disgorgement damages associated with NYU's maintenance and use of Plaintiff's and Class Members' data for its benefit and profit.

14. Through this action, Plaintiff seeks to remedy these injuries on behalf of herself and all similarly situated individuals whose Private Information was exposed and compromised in the Data Breach.

15. Plaintiff brings this action against NYU and asserts claims for negligence, breach of implied contract, unjust enrichment, and declaratory and injunctive relief.

JURISDICTION AND VENUE

16. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiff (and many members of the Nationwide Class) are citizens of states different than Defendant.

17. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business and headquarters are in New York, NY. Defendant also regularly conducts substantial business in New York.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

PARTIES

19. Plaintiff Jennie Whalen is a natural person, resident, and citizen of Manhattan, NY.

20. Defendant New York University is a tax-exempt organization under section 501(c)(3) of the Internal Revenue Code with its principal place of business located at 70 Washington Square South, New York, NY 10012.

FACTUAL ALLEGATIONS

Defendant Collected and Stored the Private Information of Plaintiff and Class Members

21. NYU is the largest private research university in the United States, educating over 65,000 students.[4]

22. Plaintiff and Class Members provided their Private Information to NYU as a requirement to obtain educational services from Defendant.

23. NYU collects Private Information from Plaintiff and Class Members such as their names, test scores, majors, ZIP codes, citizenship statuses, student application statuses, financial aid information, and financial details in the ordinary course of business. Upon information and belief, this Private Information is then stored on Defendant's systems.

24. Because of the highly sensitive and personal nature of the information NYU acquires and stores, NYU knew or reasonably should have known that it must comply with industry standards related to data security and all federal and state laws protecting Private Information and provide adequate notice if Private Information is disclosed without proper authorization.

25. Plaintiff and Class Members provided their Private Information to NYU as a condition of receiving services from NYU, but in doing so, expected NYU to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

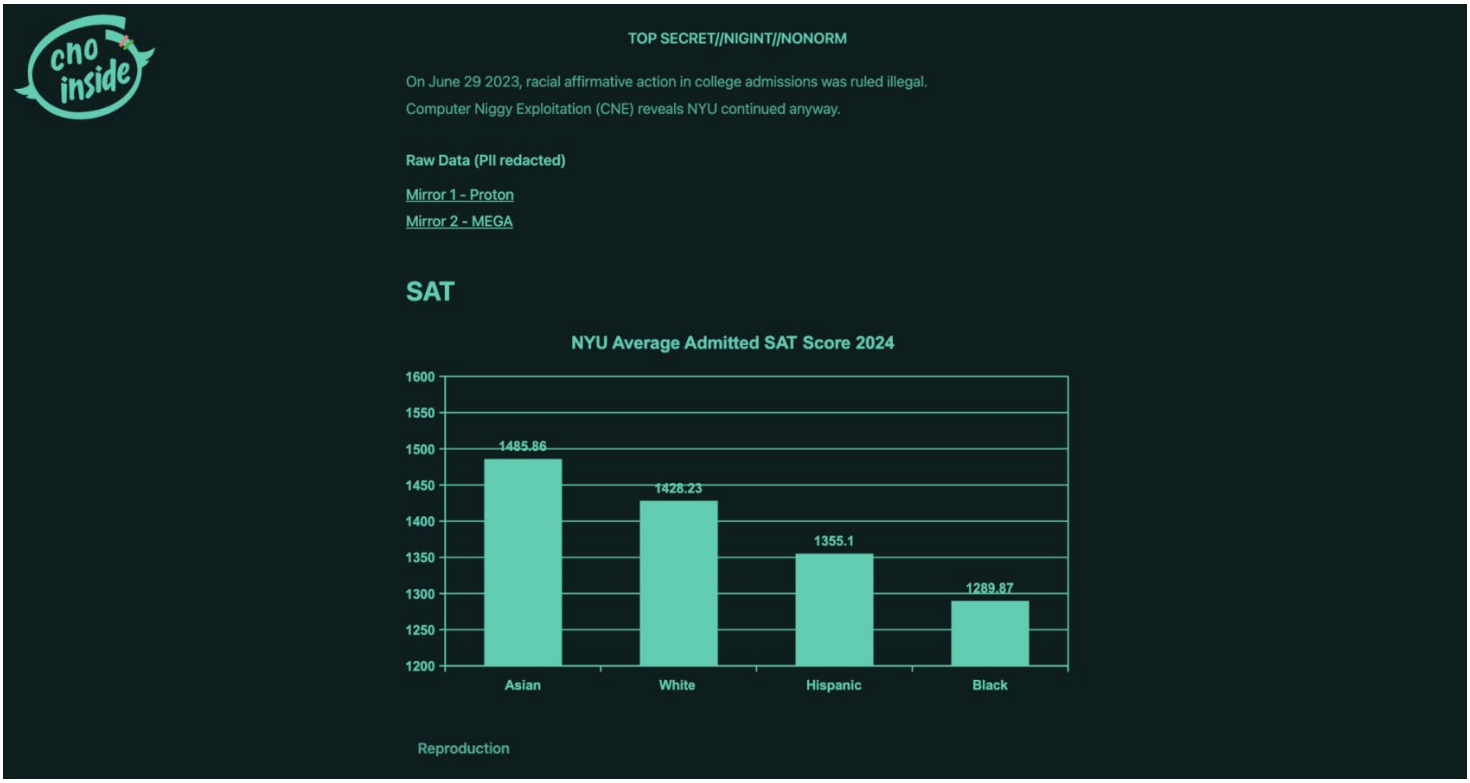
The Data Breach

[4] *About NYU*, NYU, https://www.nyu.edu/about.html (last accessed Apr. 8, 2025)

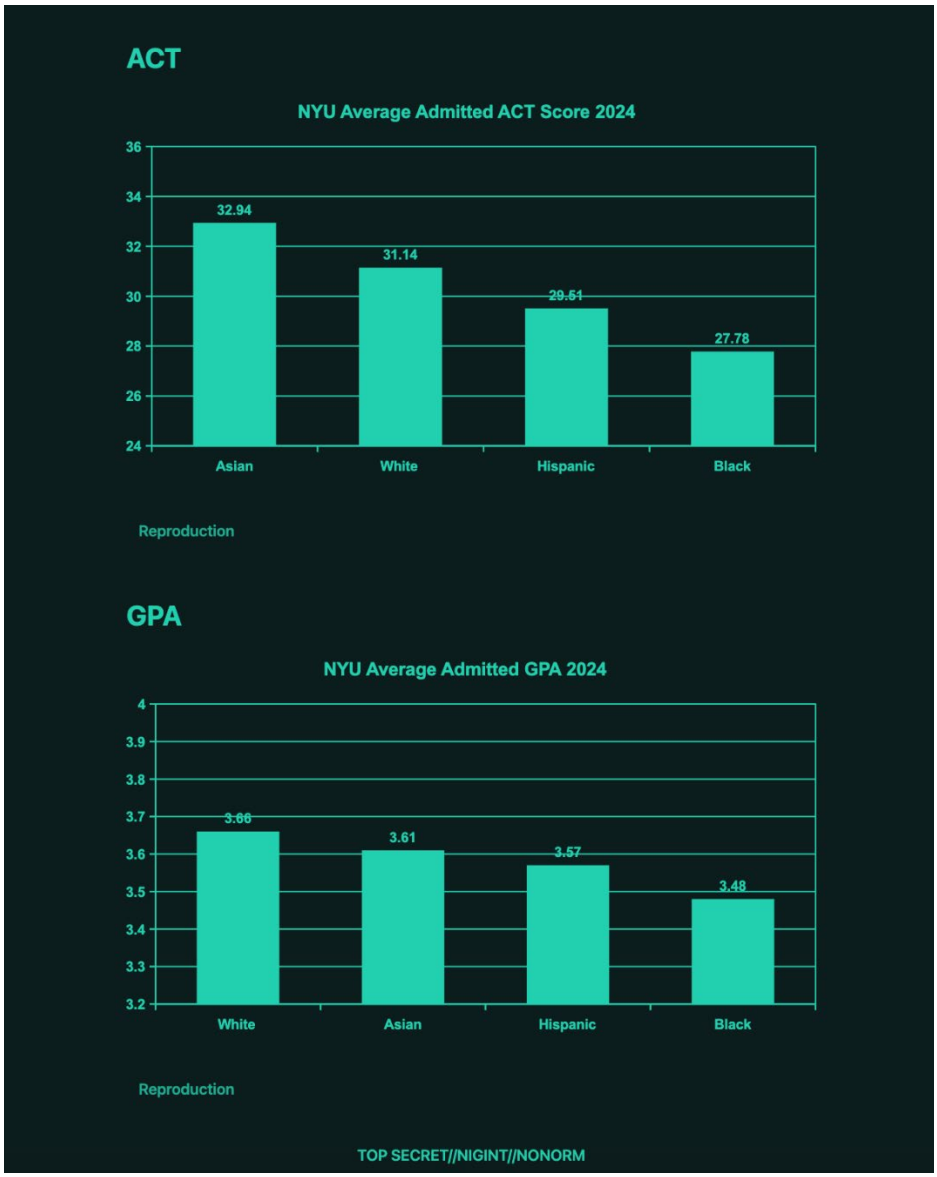
26. On or about March 22, 2025, a cybercriminal connected to cybercrime group "Computer Niggy Exploitation" gained unauthorized access to NYU's web infrastructure and stole control of systems responsible for sending internet traffic to the university's public website.[5]

27. For about two hours, NYU's online homepage was redirected to a webpage with a message referring to the United States Supreme Court's June 29, 2023 opinion striking down race-conscious admissions policies and accusing NYU of continuing to contemplate race in its admissions process.[6]

28. The hacker also posted three charts intending to show average SAT scores, ACT scores, and grade point averages ("GPA") of NYU's admitted students for the 2024-2025 admissions cycle, grouped by race. [7] Those charts are displayed below:



[5] Jonathan Greig, *Hacker Defaces NYU Website, Exposing Admissions Data on 1 Million Students*, The Record (Mar. 25, 2025), https://therecord.media/hacker-nyu-website-admissionsrace. (last accessed Apr. 8, 2025)
[6] Niles, Dev & Saadah, *supra*.
[7] *Id*.



29. The NYU homepage included links to datasets containing sensitive data on NYU applicants dating back to at least 1989.[8]

30. One cybersecurity expert, Zack Ganot, noted that the compromised data was not redacted properly and that the data included names, email addresses, home addresses, phone

[8] *Id.*

numbers, GPAs, citizenship status, financial aid details, and family member information for over one million applicants.[9] The expert characterized the Data Breach as "reckless," explaining that "[t]he collateral damage is real — and the privacy consequences for over 1 million people won't just disappear after the headlines fade." [10]

31. Despite the fact that, at the time of the Data Breach, NYU officials had been on notice of similar breaches implicating other institutions, including Georgetown University and Stanford University, NYU failed to preclude unauthorized access to NYU's systems storing sensitive data about Plaintiff and Class Members.

NYU's Response to the Data Breach

32. On or about March 27, 2025, NYU began sending victims of the Data Breach (including Plaintiff and Class Members) a message, updating them on the Data Breach ("Community Message"). The Community Message reads, in pertinent part:

> On Saturday morning, someone accessed NYU's IT systems without authorization and took control of the systems that direct web traffic to NYU's website. For a period of about three hours, traffic to the www.nyu.edu website was instead directed to a webpage that the unauthorized actor posted on GitHub. The March 22 incident at NYU appears to involve the same actor involved in a similar incident at another university.
>
> The University, which is committed to safeguarding its IT systems and to protecting personal data, responded immediately, working with a cybersecurity specialist consultant to regain control of the system and redirect traffic back to its real website. We promptly reported the incident to law enforcement authorities. And the webpage that the unauthorized actor created was taken down. The work of NYU's IT unit and the cybersecurity consultant continues, focusing on ensuring that our computer network is secure, evaluating the nature and scope of the incident, and using those findings to assess potential enhancements to NYU's cybersecurity infrastructure. They are working as swiftly as possible to complete their review so that NYU can provide notice, in accordance with applicable law, with respect to personal information that was subject to unauthorized access in connection with this incident. The law enforcement investigation also continues.[11]

[9] Hacker Defaces NYU Website, Exposing Admissions Data on 1 Million Students, *supra*.
[10] *Id*.
[11] Message to the NYU Community about the March 22, 2025, Cybersecurity Incident, *supra*.

33. Upon information and belief, Plaintiff's and Class Members' affected Private Information at the time of the Data Breach was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

34. Upon information and belief, NYU was a target due to its status as an entity that collects, creates, and maintains Private Information.

35. The Community Message gives no details to Plaintiff or Class Members regarding the manner and means of how their Private Information was disclosed and leaves Plaintiff and Class Members wondering how they can protect themselves.

36. Time is of the essence when highly sensitive Private Information is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired Private Information of Plaintiff and Class Members is now likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Private Information to criminals.

37. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Private Information, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Social Security numbers and/or specific, sensitive medical information.

38. NYU largely put the burden on Plaintiff and Class Members to take measures to protect themselves from identity theft and fraud.

39. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protection services for their respective lifetimes.

40. Plaintiff and the Class Members remain in the dark regarding exactly what data was stolen, the particular method of disclosure, the results of any investigations, and what steps are being taken, if any, to secure their Private Information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

41. NYU could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers and systems, generally, as well as Plaintiff's and Class Members' Private Information.

42. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

43. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.4% are salaried.[12]

44. According to the American Time Use Survey, American adults have between 4 to 6 hours of "leisure time" outside of work per day;[13] examples of leisure time include partaking in

[12] *Characteristics of minimum wage workers, 2022*, U.S. Bureau of Labor Statistics (Aug. 2023), https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm (last accessed on Aug. 6, 2024).
[13] *Americans have no idea how to use their free time*, Business Insider (Mar. 26, 2024), https://www.businessinsider.com/americans-free-time-leisure-dont-use-television-2024-3 (last accessed on Aug. 6, 2024).

sports, exercise and recreation; socializing and communicating; watching TV; reading; thinking/relaxing; playing games and computer use for leisure; and other leisure activities.[14] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

45. Plaintiff and Class Members are deprived of the choice as to how to spend their valuable free hours and therefore seek renumeration for the loss of valuable time as another element of damages.

The Value of PII

46. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[15]

47. In October 2023, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "malicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated victim

[14] *Table 11A. Time spent in leisure and sports activities for the civilian population by selected characteristics, averages per day, 2022 annual averages*, U.S. Bureau of Labor Statistics (June 22, 2023), https://www.bls.gov/news.release/atus.t11A.htm (last accessed on Aug. 6, 2024).

[15] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNet (Apr. 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 17, 2024).

data and pressured victims to pay by threatening to release the stolen data."[16]

48. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

49. Malicious actors can use stolen personal information to, *inter alia*, create synthetic identities (which are harder for authorities to detect), execute credible phishing attacks, and sell the personal information on underground markets in the dark web.[17]

50. Another example is when the U.S. Department of Justice announced its seizure of RaidForums in 2022. RaidForums was an online marketplace popular for cybercriminals to purchase and sell hacked data belonging to millions of individuals around the world.[18] "One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[19]

51. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. According to Prey, a company that develops device tracking and recovery software, stolen PII and can be worth up to $2,000.00 depending on the type of information

[16] *See StopRansomware Guide*, U.S. Cybersec. and Infrastructure Sec. Agency (Oct. 2023), https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf. (last accessed Apr. 8, 2025)
[17] *What Data Do Cybercriminals Steal? (How To Protect Yours)*, Identity Guard (Feb. 14, 2024), https://www.identityguard.com/news/what-information-do-cyber-criminals-steal. (last accessed Apr. 8, 2025)
[18] *United States Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator*, U.S. Dept. of Justice (Apr. 12, 2022), https://www.justice.gov/opa/pr/united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator. (last accessed Apr. 8, 2025)
[19] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor (Apr. 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/. (last accessed Apr. 8, 2025)

obtained.[20]

52. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. Such fraudulent uses include opening fraudulent credit cards and bank accounts, filing or collecting tax returns, accessing government benefits, applying for loans, and receiving healthcare. "If not spotted and resolved, these types of identity theft can rack up financial debt and do extensive damage to a person's credit, making things like obtaining a loan to buy a car or house difficult or even impossible."[21]

53. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

54. Even then, a new Social Security number may not be effective. "When issuing a new SSN, the Social Security Administration (SSA) links your old number to your new one so you'll still be associated with all wages earned."[22]

55. Because of this, the information compromised in the Data Breach here is significantly more harmful to lose than other types of data because the information compromised in this Data Breach is difficult, if not impossible, to change.

56. The PII compromised in the Data Breach also demands a much higher price on

[20] Juan Hernandez, *The Lifecycle of Stolen Credentials on the Dark Web*, Prey (Feb. 26, 2024), https://preyproject.com/blog/lifecycle-stolen-credentials-dark-web.

[21] *What to do if someone has your Social Security number*, AllState (Jan. 24, 2024), https://www.allstateidentityprotection.com/content-hub/stolen-social-security-number.

[22] *What Happens if I Change My Social Security Number*, LendingTree (Mar. 15, 2023), https://www.lendingtree.com/credit-repair/credit-score-after-getting-a-new-social-security-number/.

the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[23]

57. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

58. According to the FBI's Internet Crime Complaint Center (IC3) 2023 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $12.5 billion in losses to individuals and business victims.[24]

59. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

60. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

61. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's

[23] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells- for- 10x- price-of-stolen-credit-card-numbers.html (last visited Jan. 17, 2024).
[24] *2023 Internet Crime Report*, Fed. Bureau of Investig. (2023), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (last accessed Apr. 11, 2024).

name.[25] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[26]

62. The exposure of Plaintiff's and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

Defendant Failed to Comply with the FTC Act and Failed to Observe Reasonable and Adequate Date Security Measures

63. The FTC has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[27]

64. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[28]

---

[25] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf (last visited Jan. 17, 2024).

[26] *Id*.

[27] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

[28] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 17, 2024).

65. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

66. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[29]

67. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

68. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

69. Plaintiff and Class Members gave their PII to Defendant with the reasonable expectation and understanding that Defendant would comply with its duty to keep such information confidential and secure from unauthorized access.

[29] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

70. Defendant NYU stated in its "Digital Privacy Statement" the following representations about the supposed privacy of Plaintiff's and Class Members' Private Information:

> New York University (NYU) is committed to respecting your privacy. This privacy statement governs the collection and use of information collected through official NYU websites and other NYU digital properties.
>
> **[...]**
>
> **Security**
> NYU has implemented reasonable physical, technical, and administrative procedures to safeguard and secure all information we collect online against loss, misuse, or alteration of the information under our control. This includes the use of encryption when collecting or transferring sensitive data such as credit card information. Please note that while we work hard to protect the security of your information, NYU cannot provide an absolute guarantee as to the security of any information you transmit through our websites or digital properties, and that you do so at your own risk.[30]

71. Defendant has been on notice for years that Plaintiff's and Class Members' PII was a target for bad actors because of, among other motives, the high value of the PII created, collected, and maintained by Defendant.

72. Despite such awareness, Defendant failed to impose and maintain reasonable and appropriate data security controls to protect Plaintiff's and Class Members' PII from unauthorized access that Defendant should have anticipated and guarded against.

73. Defendant was fully aware of its obligation to protect the PII of its customers because of its collection, storage, and maintenance of PII. Defendant was also aware of the significant consequences that would ensue if it failed to do so because Defendant collected, stored,

[30] *Digital Privacy Statement*, NYU, https://www.nyu.edu/footer/copyright-and-fair-use/digital-privacy-statement.html (last accessed Apr. 8, 2025).

and maintained sensitive private information from millions of individuals and knew that this information, if hacked, would result in injury to Plaintiff and Class Members.

74. Despite understanding the consequences of insufficient data security, Defendant failed to adequately protect Plaintiff's and Class Members' PII, permitting bad actors to access and misuse it.

Defendant Failed to Comply with Industry Standards

75. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[31] All organizations collecting and handling PII, such as Defendant, are strongly encouraged to follow these controls.

76. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[32]

77. Several best practices have been identified that a minimum should be implemented by entities like Defendant, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining

[31] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), available at https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Jan. 17, 2024).
[32] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Jan. 17, 2024).

network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[33]

78. Other best practices have been identified that a minimum should be implemented by entities like Defendant, including but not limited to ensuring that PII is only shared with third parties when reasonably necessary and that those vendors have appropriate cybersecurity systems and protocols in place.[34]

79. Defendant failed to follow these and other industry standards to adequately protect the PII of Plaintiff and Class Members.

The Data Breach Caused Harm and Will Result in Additional Fraud

80. Without detailed disclosure to the victims of the Data Breach, individuals whose PII was compromised by the Data Breach, including Plaintiff and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of their PII for months without being able to take available precautions to prevent imminent harm.

81. The ramifications of Defendant's failure to secure Plaintiff's and Class Members' data are severe.

82. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

83. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[35] The FTC describes "identifying

[33] *See* Center for Internet Security, *Critical Security Controls* (May 2021), available at https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Jan. 17, 2024).
[34] *See id*.
[35] 17 C.F.R § 248.201 (2013).

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[36]

84. Identity thieves can use PII, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

85. As demonstrated herein, these and other instances of fraudulent misuse of the compromised PII has already occurred and are likely to continue.

86. Javelin Strategy and Research reports that identity thieves have stolen $43 billion in 2022.[37]

87. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. According to Experian, a credit monitoring company, "it takes an average of six months and roughly 200 hours of work to recover your identity after it's been compromised."[38]

88. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

---

[36] *Id*.

[37] *See Identity Fraud Losses Totaled $43 Billion in 2022, Affecting 40 Million U.S. Adults*, Javelin (Mar. 28, 2023), https://javelinstrategy.com/press-release/identity-fraud-losses-totaled-43-billion-2022-affecting-40-million-us-adults .

[38] Gayle Soto, *The Unexpected Costs of Identity Theft*, Experian (Sept. 30, 2020), https://www.experian.com/blogs/ask-experian/what-are-unexpected-costs-of-identity-theft/

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[39]

89. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

Plaintiff's Experience with the Data Breach

90. Plaintiff Jennie Whalen, an alumnus of NYU, provided her PII to Defendant—including her name, email address, home address, phone number, GPA, citizenship status, financial aid details, and family member information —and upon information and belief, that PII was stored and maintained by Defendant.

91. Plaintiff received a "Community Message" from Defendant notifying her of the Data Breach and of the unauthorized exposure of Plaintiff's PII.

92. Plaintiff values her privacy and makes every effort to keep her personal information private.

93. Since the Data Breach, Plaintiff has experienced a significant increase in the frequency of spam telephone calls and emails from individuals who have clearly obtained Plaintiff's private information.

94. Plaintiff is now forced to live with the anxiety that Plaintiff's PII is being disclosed to the entire world, thereby subjecting Plaintiff to embarrassment and depriving Plaintiff of any right to privacy whatsoever.

95. As a result of the Data Breach, Plaintiff has had to spend over five (5) hours dealing with the consequences of the Data Breach. This time and effort spent by Plaintiff consists of:

[39] GAO, *Report to Congressional Requesters*, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited Jan. 17, 2024).

monitoring accounts to detect suspicious and fraudulent activity to mitigate against potential harm; researching the potential consequences of the Data Breach; locking Plaintiff's credit account with Experian, TransUnion, and Equifax after finding out that Plaintiff's PII was detected on the dark web; and going to and consulting Plaintiff's bank about the Data Breach, potential data theft and precautions to be taken.

96. Plaintiff remains at a substantial and imminent risk of future harm given the highly-sensitive nature of the information stolen. Plaintiff faces a substantial risk of out-of-pocket fraud losses, such as loans opened in Plaintiff's name, medical services billed in Plaintiff's name, tax return fraud, utility bills opened in Plaintiff's name, credit card fraud, and similar identity theft.

Plaintiff and Class Members Suffered Damages

97. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

98. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented intrusion into its information storage and security systems and, ultimately, the theft of the PII of over 3 million individuals.

99. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have already been harmed by the

fraudulent misuse of their PII, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

100. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their PII;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market; and,

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

101. While Plaintiff's and Class Members' PII has been stolen, Defendant continues to hold Plaintiff's and Class Members' PII. Particularly because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

102. Plaintiff brings this class action individually and on behalf of all similarly situated persons under Federal Rule of Civil Procedure 23. Plaintiff seeks certification under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3) of the following Nationwide Class (the "Class"):

> All persons in the United States who received a notice of the Data Breach Data Breach announced by Defendant NYU to the public on March 27, 2025.

103. The Class defined above is readily ascertainable from information in Defendant's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

104. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or their parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

105. Plaintiff reserves the right to amend or modify the Class definitions as this case progresses.

106. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

107. **Numerosity**. Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of the approximately 3 million individuals whose PII and PHI were compromised by Defendant's Data Breach.

108. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. If Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. If Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If Defendant owed a duty to Class Members to safeguard their PII;

f. If Defendant breached its duty to Class Members to safeguard their PII ;

g. If Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. If Defendant should have discovered the Data Breach earlier;

i. If Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If Defendant's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

k. If Defendant's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

l. If Defendant's conduct was negligent;

m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

n. If Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

o. If Defendant breached implied contracts with Plaintiff and Class Members;

p. If Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

q. If Defendant failed to provide notice of the Data Breach in a timely manner, and;

r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

109. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, Plaintiff and Class Members were subjected to Defendant's uniformly illegal and impermissible conduct.

110. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's counsel is competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

111. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' data was stored on the same computer system and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

112. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is

superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

113. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

114. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

115. Likewise, particular issues under Federal Rule of Civil Procedure 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

116. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE

(On Behalf of Plaintiff and the Class)

117. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 119 of the Complaint as if fully set forth herein.

118. NYU required Plaintiff and Class Members to provide Defendant with PII to receive Defendant's products and services.

119. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, NYU owed a duty of care to use reasonable means to secure and safeguard their computer system—and Plaintiff's and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes so it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

120. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would at some point try to access Defendant's databases of PII.

121. After all, PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to them.

122. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

123. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and Class Members, which is recognized by laws and regulations including but not limited to the FTC Act, state statutory law, and common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

124. Defendant failed to take appropriate measures to protect the PII of Plaintiff and the Class. Any purported safeguards that Defendant had in place were wholly inadequate.

125. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches across several industries, and allowing unauthorized access to Plaintiff's and the other Class Members' PII.

126. The failure of Defendant to comply with industry and federal regulations evinces Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII.

127. But for Defendant's wrongful and negligent breach of their duties to Plaintiff and the Class, PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Class and all resulting damages.

128. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PII. Defendant knew or should have known that their

systems and technologies for processing and securing the PII of Plaintiff and the Class had security vulnerabilities.

129. As a result of this misconduct by Defendant, the PII and other sensitive information of Plaintiff and the Classes was compromised, placing them at a greater risk of identity theft and their PII being disclosed to third parties without the consent of Plaintiff and the Class.

130. As a direct and proximate result of NYU's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in NYU's possession and is subject to further unauthorized disclosures so long as NYU fails to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by NYU's data breach; (x) the value of the unauthorized access to their PII permitted by Defendant; and (xi) any nominal damages that may be awarded.

131. As a direct and proximate result of NYU's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses including nominal damages.

132. NYU's negligent conduct is ongoing, in that it still possesses Plaintiff's and Class Members' PII in an unsafe and insecure manner.

133. Plaintiff and Class Members are entitled to injunctive relief requiring NYU to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

134. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 119 of the Complaint as if fully set forth herein.

135. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving Defendant's products and services.

136. Plaintiff and Class Members entrusted their PII to Defendant. In doing so, Plaintiff and the class entered into implied contracts with Defendant by which it agreed to safeguard and protect such information to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the class if their data had been breached and compromised or stolen.

137. In entering into the implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards, and that Defendant would thoroughly vet and select vendors that adequately protect PII.

138. Implicit in the agreement between Plaintiff and Class Members and Defendant was Defendant's obligation to: (a) take reasonable steps to safeguard that PII, including through proper vetting of third party vendors to whom PII is provided; (b) prevent unauthorized disclosure of the

PII; (c) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (d) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses; and (e) retain or allow third parties to retain PII only under conditions that kept such information secure and confidential.

139. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing. Defendant required Plaintiff and Class Members to provide their PII as a condition of receiving Defendant's products and services. Plaintiff and Class Members accepted the offers and provided their PII.

140. In accepting the PII, Defendant understood and agreed that it was required to reasonably safeguard and otherwise ensure protection of the PII from unauthorized access or disclosure.

141. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant that Defendant would keep and require the third-party vendors it selects to house PII to keep, their PII reasonably secure.

142. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor and ensure that the PII entrusted to it would remain protected by reasonable data security measures and remain confidential, either in the hands of Defendant or one of its vendors.

143. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant by providing their PII at Defendant's request.

144. Defendant breached the implied contracts made with Plaintiff and the class by failing to safeguard and protect their PII, by entrusting the PII to a vendor that fails to safeguard

PII, by failing to delete the PII of Plaintiff and the Class or requiring vendors to delete information once the relationship ended, and by failing to provide accurate notice to them that their PII was compromised as a result of the Data Breach.

145. As a direct and proximate result of Defendant's breach of these implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

146. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

147. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data monitoring procedures; (ii) evaluate, audit, and improve its processes for vetting third party vendors and the selection processes for vendors to which Defendant provides sensitive PII; (iii) submit to future annual audits of those systems and monitoring procedures; (iv) bolster its IT security measures; and (v) immediately provide or continue providing adequate credit monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

148. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 119 of the Complaint as if fully set forth herein.

149. Plaintiff and Class Members conferred a benefit on Defendant by entrusting their PII to Defendant from which it derived profits.

150. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead

calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide adequate security.

151. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

152. Defendant acquired the PII through inequitable means in that Defendant failed to disclose the inadequate security practices, previously alleged, and failed to maintain adequate data security.

153. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to disclose their data to Defendant.

154. Plaintiff and Class Members have no adequate remedy at law.

155. As a direct and direct an proximate result of NYU's conduct, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in NYU's possession and is subject to further unauthorized disclosures or further entrustment to inadequate third party vendors so long as NYU fails to undertake appropriate and adequate measures to protect the PII; (vii) future costs in terms of time, effort and money that will be expended to prevent,

detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by NYU's data breach; (x) the value of the unauthorized access to their PII permitted by Defendant; and (xi) any nominal damages that may be awarded.

156. Plaintiff and Class Members are entitled to restitution and/or damages from NYU and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by NYU from its wrongful conduct, as well as return of their sensitive PII and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

157. Plaintiff and Class Members may not have an adequate remedy at law against NYU, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

158. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 119 of the Complaint as if fully set forth herein.

159. Defendant became the guardian of Plaintiff's and Class Members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of Plaintiff's and Class Members' PII, to act primarily for their benefit. This duty included the obligation to safeguard Plaintiff's and Class Members' PII and to timely detect and notify Plaintiff and Class Members in the event of a data breach.

160. Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiff's and Class Members' PII for the benefit of Plaintiff and Class Members in

order to provide Defendant's products and services to Plaintiff and Class Members.

161. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members within the scope of its relationship with them. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to properly protect PII. Defendant further breached its fiduciary duties by failing to timely detect the Data Breach and notify and/or warn Plaintiff and Class Members of the Data Breach.

162. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as it fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of the PII compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

163. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or

harm, and other economic and non-economic losses.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

164. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 119 of the Complaint as if fully set forth herein.

165. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

166. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and Class Members continue to suffer injuries as result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

167. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (a) Defendant owes a legal duty to secure PII and to timely notify impacted individuals of a data breach under the common law, Section 5 of the FTC Act, and various state statutes, and (b) Defendant continues to breach this legal duty by failing to employ reasonable measures to secure PII in its possession.

168. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to

protect PII in Defendant's possession and control.

169. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at NYU occurs, Plaintiff and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

170. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

171. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and Class members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, on behalf of herself and all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as the Class Representative;

B. A mandatory injunction directing Defendant to adequately safeguard the PII of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII ;

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised,

hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to monitor ingress and egress of all network traffic;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xi. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII ;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Complaint so triable.

Dated: April 9, 2025

GLANCY PRONGAY & MURRAY LLP

By: */s/ Brian Murray*
Brian P. Murray (BM 9954)
230 Park Avenue, Suite 358
New York, NY 10169
Phone. (212) 682-5340
bmurray@glancylaw.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A.Yanchunis *
Ronald Podolny
Antonio Arzola, Jr. *
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Phone: (813) 275-5272
Fax: (813) 222-4736
jyanchunis@forthepeople.com
ronald.podolny@forthepeople.com
ararzola@forthepeople.com

*****_Pro hac vice forthcoming_

Counsel for Plaintiff and the Class

.